In the Claims:

1. (Original) A method of protecting a program memory device including program memory content, wherein the program memory content is associated with a previously stored signature, the method comprising:

automatically disconnecting the program memory device from a control device that is operationally dependent upon the program memory device;

halting the control device;

verifying whether a present signature is equivalent to the previously stored signature to obtain a verification result; and

based on the verification result, performing one of:

disabling reading and writing of the program memory device; or

automatically reconnecting the program memory device to the control device.

2. (Original) The method of Claim 1, wherein the step of verifying comprises:

independently computing a binary content verification of the program memory content; and

comparing the previously stored signature with the binary content verification.

3. (Original) The method of Claim 1, wherein the step of independently computing the binary content signature comprises storing the binary content signature in a secure memory device physically separated from the program memory and not accessible by the control device.

4. (Original) The method of Claim 3, wherein the secure memory device is a securely enclosed unit that is tamperproof and that has electrical connections available for connection with the program memory device.

5. (Original) The method of Claim 1, wherein the binary content signature is a binary bit-for-bit copy of the program memory content of the first time period, and the binary content verification is another binary bit-for-bit copy of the program memory content of the second time period.

6. (Original) The method of Claim 1, wherein the protecting is performed automatically and without manual intervention.

7. (Original) The method of Claim 1, wherein the protecting is performed dynamically while the program memory device is being accessed by the control device.

8. (Original) The method of Claim 7, wherein the step of disabling reading and writing of the program memory chip comprises maintaining control device stability.

9. (Original) The method of Claim 1, further comprising:

disabling reading and writing of a first portion of the program memory device; and

maintaining a second portion of the program memory device in an active state.

10. (Original) The method of Claim 1, wherein the step of disabling reading and writing of the program memory device comprises preventing unauthorized programming of the program memory device.

11. – 35. (Cancel)

36. (New) A consumer interactive device, comprising:

a processing unit configured to administer use of the consumer interactive device;

a display coupled to the processing unit and utilized by the processing unit to display portions of the use of the consumer interactive device;

a memory unit coupled to the processing unit;

a set of instructions and/or data for use of the consumer interactive device stored in the memory unit;

a signature calculator independent of the processing unit, the signature calculator coupled to the memory unit and configured to produce a signature from contents of the memory unit;

a signature storage memory coupled to the signature calculator and configured to store a signature produced by the signature calculator; and

a memory unit protection module configured to compare a current signature produced from the current contents of the memory unit, compare the current signature to a previously produced signature and, if the signatures do not match, de-couple the memory unit from the processing unit.

37. (New) The consumer interactive device according to Claim 36, wherein the signature calculator, the signature storage memory, and the memory unit protection module are disposed in a secure memory socket having receptacles to receive pins of the memory unit.

38. (New) The consumer interactive device according to Claim 36, wherein the consumer interactive device is a casino gaming machine.

39. (New) The consumer interactive device according to Claim 36, wherein the consumer interactive device is an ATM machine.

40. (New) The consumer interactive device according to Claim 36, wherein the memory protection unit is further configured to communicate with a remote verification unit utilized to verify the memory contents to a floor manager or agent.

41. (New) The consumer interactive device according to Claim 36, wherein the consumer interactive device is a gaming machine and the memory protection unit is further configured to communicate with a remote verification unit utilized to verify the memory contents by a floor agent according to gaming regulations.

42. (New) The consumer interactive device according to Claim 36, further comprising a data read port coupled to the memory unit protection module and configured to communicate a verification of the memory unit to a check device external to the consumer interactive device.

43. (New) The consumer interactive device according to Claim 36, wherein the memory protection unit is independent of the processing unit.

44. (New) The consumer interactive device according to Claim 36, wherein the signature memory is independent of the program memory.

45. (New) A casino gaming unit, comprising:

a processing unit;

a memory unit coupled to the processing unit;

a data read port accessible from a portion of the gaming unit not physically accessible to the memory unit and configured to allow verification of contents of the memory unit.

46. (New) The casino gaming unit according to Claim 45, wherein the data read port is a wireless access point.

47. (New) The casino gaming unit according to Claim 45, further comprising a portable remote access device configured to access the wireless access port, calculate a signature of contents of the memory unit, compare the signature to a previous signature stored on the remote access device.

48. (New) The casino gaming unit according to Claim 46, further comprising a remote access unit configured to access the wireless access port, calculate a signature of contents of the memory unit, compare the signature to a previously stored signature.

49. (New) The casino gaming unit according to Claim 48, wherein the remote access device is further configured to access a plurality of addition wireless access points each corresponding to a respective one of a set of additional gaming units and check memory contents of each of the additional gaming machines against previously stored signatures.

50. (New) The casino gaming unit according to Claim 45, wherein the verification of contents of the memory unit comprises a verification of a signature of contents of a memory unit storing programs and/or data used by a gaming processor to implement the casino gaming unit, and the verification is performed by a processing unit independent from the gaming processor.

51. (New) The casino gaming unit according to Claim 50, wherein the verification comprises a comparison of the signature with a previously computed signature stored in a secure memory module not accessible to the gaming processor.

52. (New) A casino gaming apparatus, comprising

a physically secure, locked, enclosure comprising a processing unit coupled to program memory configured to operate the casino gaming unit, the program memory comprising contents including instructions and/or data utilized by the processing unit;

a program memory verification unit coupled to the program memory and configured to calculate a signature of the program memory contents and verify the calculated signature against the previously calculated signature;

a secure memory, comprising,

an IC memory device physically separated and distinct from the program memory, and accessible only by the program verification unit; and

a Radio Frequency (RF) device coupled to the program verification unit and configured to transmit the verification result to a monitor;

wherein the previously calculated signature is stored in the secure memory.

53. (New) The casino gaming apparatus according to Claim 52, wherein the monitor comprises a Remote Monitory Unit (RMU).

54. (New) The casino gaming apparatus according to Claim 52, wherein the program verification unit and the secure memory are contained in a socket in which the program memory is installed.

55. (New) The casino gaming apparatus according to Claim 52, wherein the program verification unit is further configured to decouple the program memory from the processing when the calculated signature does not match the previously calculated and stored signature.

56. (New) The casino gaming apparatus according to Claim 52, wherein the program verification unit is further configured to decouple the program memory from the processing unit and feed a predetermined set of instructions to the

processing unit when the calculated signature does not match the previously calculated and stored signature.

57. (New) The casino gaming apparatus according to Claim 56, wherein the predetermined set of instructions comprises no-op instructions.

58. (New) The casino gaming apparatus according to Claim 52, wherein the casino gaming apparatus is a slot machine.

59. (New) The casino gaming apparatus according to Claim 52, wherein:

the program memory is installed on a circuit board using a plug-in type socket that removably holds and connects the program memory to the circuit board in a manner that allows it to be readily removed and re-installed; and

the secure memory is installed in the apparatus in a permanent and nonremovable way such that is not readily removed and reinstalled.

60. (New) The casino gaming apparatus according to Claim 52, wherein the program memory verification unit is independent of the processing unit.

61. (New) A secure memory socket, comprising,

a socket device having receptacles positioned to receive pins of a memory unit;

a set of data and control pins coupled to portions of the receptacles and configured to carry data from a memory unit installed in the socket device to a processor device to be coupled to the data and control pins;

a signature calculator coupled to the receptacles and configured to produce a signature from contents of the memory unit,

a signature storage memory coupled to the signature calculator and configured to store a signature produced by the signature calculator, and

a memory unit protection module configured to compare a current signature produced from current contents of the memory unit, compare the current signature to a previously produced signature from the signature storage memory, and, if the signatures do not match, de-couple the receptacles from at least a portion of the pins.

62. (New) The secure memory socket all to Claim 61, wherein the signature calculator, signature storage memory, and memory unit protection module are implemented within a single IC package enclosure comprising a body of the socket device.

63. (New) The secure memory socket according to Claim 61, further comprising a Radio Frequency (RF) device coupled to the memory unit protection module and configured to communicate results of the comparison to a monitoring device.

64. (New) The secure memory socket according to Claim 63, wherein the RF device, the signature calculator, signature storage memory, and memory unit protection module are implemented within a single IC package enclosure comprising a body of the socket device.

65. (New) The secure memory socket according to Claim 61, wherein the memory unit protection unit is further configured to feed a set of microprocessor disabling instructions to at least one of the data and control pins upon decoupling of the receptacles.

66. (New) The secure memory socket according to Claim 61, wherein wherein the memory unit protection unit is further configured to place a disable pattern on a data bus to the processor device.

67. (New) A method, comprising the steps of:

calculating a first signature from the contents of a program memory in consumer interactive device;

storing the program memory contents signature in a signature memory that is a different and physically separate memory from the program memory;

receiving a command from a Remote Monitor Unit (RMU) to verify contents of the program memory; and

in response to the command,

calculating a second signature from the contents of the program memory,

comparing the first signature to the second signature,

if the signatures do not match, signaling a memory error to the RMU and disabling the program memory from communicating with a processing device utilizing contents of the program memory to operate.

68. (New) The method according to Claim 67, wherein:

the step of disabling comprises,

physically disconnecting the program memory from the processing device, and

inserting special operative steps in to the processor to prevent runaway of the processor.

69. (New) The method according to Claim 68, wherein the special operative steps comprise no-op instructions.

70. (New) The method according to Claim 67, wherein the RMU comprises a gaming commission field agent's handheld wireless device.

71. (New) The method according to Claim 67, wherein the RMU comprises a casino operator's monitoring device.

72. (New) The method according to Claim 67, where the signature memory is stored in a physically secure memory in electrical packaging comprising a socket in which the program memory is installed.

73. (New) The method according to Claim 67, wherein the calculating steps are performed independently of a processor utilizing the program memory contents.